UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/633,719	08/07/2000	Jerry D. Burchfiel	00-4012	3825

32127 7590 08/04/2004

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQEO3H14
IRVING, TX 75038

EXAMINER	
MOORE, IAN N	

ART UNIT	PAPER NUMBER
2661	

DATE MAILED: 08/04/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/633,719	Applicant(s) BURCHFIEL ET AL.	
	Examiner Ian N Moore	Art Unit 2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 and 18-20 is/are rejected.

7)☒ Claim(s) 17 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This is in response to amendment filed on June 1, 2004 (paper # 6).

Response to Arguments

2. Applicant's arguments with respect to **amended claims 1-16 and 18-20** have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 10 and 20, the applicant argued that, "...Sugiyama'547 does not disclose ...determining an expected port on which a packet is expected to be received..." in page 9, paragraph 2, "Sugiyama'547 does not teach or suggested determining an expected port...", "...did not find any reference in Sugiyama'547 relating to an expected port or equivalent thereof..." in page 9, paragraph 3, "...learning circuit does not provide a means for determining an expected port for a packet..." in page 10, paragraph 1.

In response to applicant's argument, the examiner respectfully disagrees that Sugiyama'547 does not disclose determining an expected port on which a packet is expected to be received. As recited in the first office action, Sugiyama'547 clearly teaches the address learning means (i.e. address learning CKT 57) which **learns the port address for distinguishing the given LAN**; see col. 2, lines 4-20, col. 4, lines 33-49. Note that the learned address (when the switched is already operating) or set address (when the switched is initialized for the first time), is used to distinguished the LAN. Thus, examiner asserts the learned address or set address as "expected port". Moreover, LAN port address setting 41 indicates that the address information corresponds to the LAN 10 side, which is the source

port address where the packet is received. As stated in col. 2, lines 28-34 described the comparing means LAN port address. Thus, it is clear that in order to perform, the learned or set address must be of the received packet must be determined and examined. Thus, it is clear that learning circuit has functionality of determining a provisioned or set port address, when working together with LAN port address setting circuit, under the control of Microprocessor 56 (see FIG. 1).

The applicant argued that, "...Sugiyama'547 the LAN port address comparing circuit compares a LAN port address corresponding with the destination, as read from a memory, with the LAN port address of the source in a setting circuit..." in page 9, paragraph 2.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., **addresses**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument, the examiner respectfully disagrees that Sugiyama'547 the LAN port address comparing circuit compares a LAN port address corresponding with the **destination**, as read from a memory, with the LAN port address of the **source** in a setting circuit. Applicant is referring to the first comparing means, where destination address of the received packet is compared against the stored source address, as stated in see col. 2, lines 21-27. As citied in the first action page 12, examiner is asserting the second comparison means, where the port address of the LAN corresponding to the

transmit-**source** (i.e. LAN 10 where the packet is received from) and the learned or set circuit source port address; see Sugiyama'547 col. 2, lines 29-34.

The applicant argued that, "...Sugiyama'547 does not teach or suggest ...comparing of an actual port with an exported port..." in page 10, paragraph 2.

In response to applicant's argument, the examiner respectfully disagrees "...Sugiyama'547 does not teach or suggest ...comparing of an actual port with an exported port. Sugiyama'547 FIG. 1, LAN port address comparing circuit 46, as recited by the first office action, compared the bench-mark, set, or previously learned transmit-**source** LAN port address with LAN port address of the newly received LAN port **source** address.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., **source or destination port**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The applicant argued that, "...Khansari'131 does not discloses a method, system, switch, and/or network comparing the actual port to the expected port, and providing the packet handling when the actual port does not correspond to the expected port...."

In response to applicant's argument, the examiner respectfully disagrees that "...Khansari'131 does not discloses a method, system, switch, and/or network comparing the actual port to the expected port, and providing the packet handling when the actual port does not correspond to the expected port...." Khansari'131 discloses a method, system, switch,

and/or network **(see FIG. 1, Bridge 12)** comparing **(Fig. 7, step 208,210)** the actual port **(col. 6, line 50-60; inbound port number)** to the expected port **(see col. 5, lines 25-52; the port number stored in the database entry table 2; note that inbound port number is compared to the port number stored in the database entry table);** and providing the packet handling when the actual port does not correspond to the expected port **(see Fig. 7, step 214; col. 6, line 60-64; a duplicate packet/traffic arrived at the switch is the faulty/erroneous packet, and it is detected by comparing according to the entry table and discarded by the switch since the received ports are not the same).**

The applicant argued that, "...Khansari'131 does not teach spurious packet handling if a spurious packet is received by Khansari'131..." in page 11, paragraph 1.

In response to applicant's argument, the examiner respectfully disagrees that "...Khansari'131 does not teach spurious packet handling if a spurious packet is received by Khansari'131..." As stated in the first office action, examiner asserts spurious packet handling as detecting or determining whether received packet are duplicated packets after comparing the port numbers, as described in Khansari'131 FIG. 7, steps 210 and 214.

Regarding claims 10 and 20, in response to applicant's argument (in pages 9-12) that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies **(i.e., expected port and actual port)** are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Note that **Claims 10 and 20 only recites, " a first port" and the "second port".**

In view of the above, **the examiner respectfully disagrees** with applicant's argument and believes that the combination of references as set forth in the 103 rejections is proper, thus, claims 10-16,18-20 are obvious over Khansari'131 in view of Sugiyama'547 for at least the reasons discussed above. Claims 1-9 are rejected Witkowski'733 in view of Khansari'131 as set forth below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1 and 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Witkowski (U.S. 6,665,733) in view of Khansari (U.S. 6,446,131).

Regarding claims 1 and 8, Witkowski'733 discloses a system **(see FIG. 1, a network switch 102 or see FIG. 6, network switch 600; see col. 13, lines 26-33)** for detecting network traffic comprising:

receiving means for receiving a packet **(see FIG. 1, a network switch 102 receives a packet)**, the packet including data for transmission **(see FIG. 1, network devices 110,114,116 and 118 are laptop, servers, DTS and any other network device which transmit data packets)** over a network **(see FIG. 1, network system 100); see col. 5, lines 27-50**;

first determining means (**see FIG. 1, port control circuitry 154 or 150**) for determining an expected port (**see col. 6, lines 44-51; an assigned port number**) for the packet upon which the packet is expected to be received (see FIG. 1; **col. 11, lines 20-23; note that when a packet from network device 110 to the port 130 is received, the port control circuitry 154 learns, assigns, and stores the port number of the port 130 to network work device 110 (i.e. address A) in the memory table);**

second determining means (**see FIG. 1, port control circuitry 154 or 150**) for determining an actual port (**see FIG. 4A, step 406 and 412; source port number**) for the packet upon which the packet is actually received (**see col. 11, lines 20-36; note that a source port number is determined in order to perform comparison**); and

comparing the actual port to the expected port (**see FIG. 4A, Step 412, compares source port number with assigned port number; see col. 11, lines 20-36**); and

handling means for providing packet handling upon determining that the actual port does not correspond to the expected port (**see FIG. 4A, step 414 and step 420; see col. 11, lines 29-46; note that when source port and assigned port does not match, the packet handling is performed by assigning the port address**).

Witkowski'733 does not explicitly disclose spurious network traffic and a spurious packet handling (**see Khansari '131 Fig. 7, step 214; col. 6, line 60-64; note that a duplicate packet arrived at the switch is the faulty/erroneous packet, and it is discarded by the switch since the received ports are not the same**).

However, this limitation is taught by Khansari '131. Witkowski'733 teaches a mechanism for processing a receiving packet at different ports. Khansari '131 teaches

discarding erroneous packet when received port is not the same. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Witkowski'733 as taught by Khansari '131 for the purpose of determining whether the frame was previously received on a port other than the inbound port; discarding the frame if the frame was previously received; see Khansari '131 col. 2, line 45-53. The motivation being that by providing a way to handle packet arriving at different port, it can increase optimal network connectivity.

Regarding claim 3, Khansari '131 discloses spurious packet handling includes discarding the packet (Fig. 7, step 214; col. 6, line 60-64; note that when a duplicate packet arrived at the switch, it is the faulty/erroneous packet, and it is discarded by the switch.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Witkowski'733 as taught by Khansari '131 for the same reason stated in Claims 1 and 8.

2. Claim 2 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Witkowski'733 and Khansari '131, as applied to claim 1 above, and further in view of Dobbins (U.S. 5,946,308).

Regarding claim 2, the combined system Witkowski'733 and Khansari '131 discloses determining an expected port for the packet; and providing spurious packet handling when the actual port does not correspond to an expected port as described above in Claim 1.

Neither Witkowski'733 nor Khansari '131 explicitly discloses a plurality of expected ports (see Dobbins '308 Fig. 1 network consists of SFPS switches and Fig. 3 a logical view of an SFPS switch; see col. 4, line 21 to col. 5, line 41; note that SEFS switches in Fig. 1 has plurality of input and output ports and each port is connected to either plurality of network sides (label N) or access sides (i.e. user side/customer side with label A). In particular SEFS switch S3 has four network ports connecting to other switches (i.e. S1 to S6). Therefore, an SEFS switch can be configured to receive a packet at any ports from other switches based upon network routing topology.)

However, this limitation is taught by Dobbins '308. The combined system of Witkowski'733 and Khansari '131 teaches Inter-LAN connection equipment that has an intelligent of which port a packet should receive. Dobbins '308 teaches that utilizing an SEFS switch with plurality of configured ports and ability to receive packets from various network/switches over the network. Thus, the combined system of Witkowski'733 and Khansari '131 can be used in Dobbins '308 network where there are pluralities of switches. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Witkowski'733 and Khansari '131, as taught by Dobbins '308, for the purpose of designing a new secure fast packet switching (SFPS) technology which provides the same or better reliability and security as routers, but with much greater performance and without an increase in cost; see Dobbins '308 col. 1, line 44-55. The motivation being that by utilizing an SEFS switch in the network, it can increase the ability to guarantee a quality of service (QOS) by providing dedicated switched paths through the network via dedicated ports.

Regarding claim 7, the combined system Witkowski'733 and Khansari '131 discloses determining an expected port for the packet as described above in Claim 1.

Neither Witkowski'733 nor Khansari '131 explicitly discloses generating a table (see Dobbins '308 Fig.6 and Fig. 7, Table 1, VLAN mapping for Switch 11), the table associating each one of a plurality of source network addresses (see Dobbins '308 Table 1, VLAN IDs: VLAN 100 and 200) with a single port (see Dobbins '308 Table 1, access port 2);

determining a source network address for the packet (see Dobbins '308 col. 6, line 46-59; note that each switch strip off the encapsulated VLAN header in order to identify VLAN address); and

applying the table to determine single port associated with the source network address, the single port being the expected port. (See Dobbins '308 col. 7, line 13-40; note that each access port is configured/determined by mapping to at least one or more corresponding VLAN. Thus, when the packet arrives at the port, the table is used to identify which VLAN does the packet belong, and the table validates whether the access port is the configured port to a received packet.)

However, this limitation is taught by Dobbins '308. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Witkowski'733 and Khansari '131, as taught by Dobbins '308, for the same reason stated above in Claim 2.

3. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Witkowski'733 and Khansari '131, as applied to claim 1 above, and further in view of Miklos (U.S. 6,621,796).

Regarding claim 4, the combined system Witkowski'733 and Khansari '131 discloses spurious packet handling as described above in Claim 1.

Neither Witkowski'733 nor Khansari '131 explicitly discloses generating an alert (see Miklos'796 Fig. 4 and col. 15, line 45-62; note that after the sender discards the packet, it generates a discard-signaling PDU message to notify the receiver which PDU has been discarded.)

However, this limitation is taught by Miklos'796. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Witkowski'733 and Khansari '131, as taught by Miklos'796, for the purpose of providing a sender-initiated discard mechanism that is specifically designed to operate efficiently and effectively with Selective Repeat ARQ; see Miklos'796 col. 2, line 55-61. The motivation being that by notifying the receiver regarding the discarded PDU, it can increase efficiency and reliability in the network.

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Witkowski'733 and Khansari '131, as applied to claim 1 above, and further in view of Kadambi (U.S. 6,104,696).

Regarding claim 5, the combined system Witkowski'733 and Khansari '131 discloses the packet as described above in Claim 1.

Neither Witkowski'733 nor Khansari '131 explicitly discloses an Internet Protocol packet (see Kadambi'696 col. 28, line 5-10; note that the router processes an IP packet or IPX packet arriving at the ingress module.)

However, this limitation is taught by Kadambi'696. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Witkowski'733 and Khansari '131, as taught by Kadambi'696, for the purpose of designing the improved processing speed Layer three switches, sometimes referred to as routers, which can forward packets based upon the destination network address, can learn addresses maintain tables thereof which correspond to port mappings, utilize specialized high performance hardware, and off loading the host CPU so that instruction decisions do not delay packet forwarding; see Kadambi'696 col. 2, line 35-44. The motivation being that by utilizing layer-3 (i.e. IP) network switch, it can improve the speed of routing since routing is fully depended on the network addresses.

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Witkowski'733 and Khansari '131, as applied to claim 1 above, and further in view of Spiegel (U.S. 5,649,108).

Regarding claim 6, the combined system of Witkowski'733 and Khansari '131 discloses an expected port for the packet further comprises: determining a source network address for the packet (**see FIG. 4A, step 408, identify source MAC address of the received packet ; see col. 11, lines 15-20);**

wherein an ending of the expected path is the expected port (**see FIG. 4A, step 406,408 and 410; note that the source port must correspond to the source address of the**

remote network device, and the packet is received via the source path, and the source path must end at the source port; see col. 11, lines 14-30).

Neither Witkowski'733 nor Khansari '131 explicitly discloses calculating a path for the packet according to the routing trees of one or more switches (See Spiegel '108 col. 6, line 37-67; note that each switch determines/calculates a path based upon the routing table.)

However, this limitation is taught by Spiegel '108. Note that Witkowski'733 teaches that determining a source port, a packet source address and the end of the source path. Spiegel '108 teaches a switch that determines/calculates a path based upon the routing table. Thus, Spiegel '108's switch can be used to determine a configured path for a packet according to the routing tables. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Witkowski'733 and Khansari '131, as taught by Spiegel '108, for the purpose of providing the best alternate paths, or the paths with the least total cost if link-state protocols are used; see Spiegel '108 col. 2, line 24-25. The motivation being that by utilizing routing information stored routing table, it can increase the reliability in the network.

6. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Witkowski'733 and Khansari '131, as applied to claim 8 above, and further in view of Dobbins (U.S. 5,946,308).

Regarding claim 9, the combined system Witkowski'733 and Khansari '131 discloses determining means for determining a expected port for the packet; and handling means for providing spurious packet handling when the actual port does not correspond to an expected port as described above in Claim 8.

Neither Witkowski'733 nor Khansari '131 explicitly discloses third determining, a plurality of expected ports, and second handling (see Dobbins '308 Fig. 1 network consists of SFPS switches and Fig. 3 a logical view of an SFPS switch; see col. 4, line 21 to col. 5, line 41; note that SEFS switches in Fig. 1 has plurality of input and output ports and each port is connected to either plurality of network sides (label N) or access sides (i.e. user side/customer side with label A). In particular SEFS switch S3 has four network ports connecting to other switches (i.e. S1 to S6). Therefore, each SEFS switch can receive a packet at any ports in from other switches based upon network and routing topology. Moreover, when a packet is received at a port, three processes occur: first configuration/determining received packet's port and address number by way of storing in the memory, second comparing/determining the received packet with the stored information, and process the packet based upon the result. Therefore, the same three processes can be repeated for the packets receiving at plurality of incoming ports (i.e. third configuration/determining and second processing).)

However, this limitation is taught by Dobbins '308. The combined system of Witkowski'733 and Khansari '131 teaches Inter-LAN connection equipment that has an intelligent of which port a packet should receive. Dobbins '308 teaches that utilizing an SEFS switch with plurality of configured ports and ability to receive packets from various network/switches over the network. Thus, the combined system of Witkowski'733 and Khansari '131 can be used in Dobbins '308 network where there are pluralities of switches. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Witkowski'733 and Khansari '131, as

taught by Dobbins '308, for the purpose of designing a new secure fast packet switching (SFPS) technology which provides the same or better reliability and security as routers, but with much greater performance and without an increase in cost; see Dobbins '308 col. 1, line 44-55. The motivation being that by utilizing an SEFS switch in the network, it can increase the ability to guarantee a quality of service (QOS) by providing dedicated switched paths through the network via dedicated ports.

7. Claims 10, 12,13,14, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khansari '131 in view of Sugiyama '547.

Regarding claim 10, Khansari '131 discloses a switch (see Fig. 2a, Bridge 16) for use in an internetwork (see Fig. 2a, internetwork between LAN 1 and LAN 3), the switch comprising: a plurality of ports (see Fig. 5, ports A1, B1, and C1), each port connected in a communicating relationship with at least one of a connected switch (see Fig.2a, Bridge 14) and a network (see Fig. 2a, network 10);

a routing database (see Fig. 5, Memory 52), the routing database containing information relating to the internetwork (see col. 6, line 1-59; see Fig. 5, Memory 52 contains a program, filtering database, and hash table 58; note that memory contains a database to store/learn reading address information regarding the packets to be switched/routed between internetwork);

a processor (**see Fig. 5, Controller 50**) further configured to provide spurious packet (see FIG. 7, a duplicate packet) handling upon determining; whereby spurious network traffic within the internetwork is detected **(see Fig. 7, step 214; col. 6, line 60-64; see col. 5, lines**

25-52; bridge 12's database entry table 2; Fig. 7, step 208,210; col. 6, line 50-60; note that inbound port number is compared to the port number stored in the database entry table. A duplicate packet/traffic arrived at the switch is the faulty/erroneous packet, and it is detected by comparing according to the entry table and discarded by the switch since the received ports are not the same);

Khansari '131 does not explicitly disclose the processor configured to compare a first port to a second port (see Fig. 1, LAN port Address Comparing CKT 46 and Terminal Address Comparing CKT 47; see col. 2, line 22-34 and col. 5, line 29-53; Examiner is asserting the second comparison means, where the port address of the LAN corresponding to the transmit-**source** (i.e. LAN 10 where the packet is received from) and the learned or set circuit source port address; see Sugiyama'547 col. 2, lines 29-34Note that when the packet is received, the comparing circuits determine the validity of a packet by comparing between receiving port and learned port. In particular, a received packet's source address, destination address and the "first" received LAN port number are compared against the information (i.e. information including a second port number) stored in Filtering Address Table memory (of) learned memory. When the packet is received at a port, Inter-LAN connection equipment determines the validity of a packet regarding receiving port number and expected port number. Therefore, it is clear that Inter-LAN connection equipment has a mechanism to identify the receiving port, which is a port where packets are arriving),

the first port of the plurality of ports through which a packet is received (see col. 2, line 22-34 and see col. 5, line 29-53; note that any port (i.e. LAN 10 port, LAN20 port, or LAN 30 port) can receive a packet, and receiving port is the "first" port), and

the second port of the plurality of ports through which the packet is expected to received (see Fig. 1, Address Learning CKT 57; see col. 2, line 4-20 and col. 4, line 33-67; Sugiyama'547 clearly teaches the address learning means (i.e. address learning CKT 57) which **learns the port address for distinguishing the given LAN**; see col. 2, lines 4-20, col. 4, lines 33-49. Note that the learned address (when the switched is already operating) or set address (when the switched is initialized for the first time), is used to distinguished the LAN. Thus, examiner asserts the learned address or set address as "expected port". Moreover, LAN port address setting 41 indicates that the address information corresponds to the LAN 10 side, which is the source port address where the packet is received. As stated in col. 2, lines 28-34 described the comparing means LAN port address. Thus, it is clear that in order to perform, the learned or set address must be of the received packet must be determined and examined. Thus, it is clear that learning circuit has functionality of determining a provisioned or set port address, when working together with LAN port address setting circuit, under the control of Microprocessor 56 (see FIG. 1). Note that each received packet's source address (SA) and its corresponding LAN port address (i.e. the port where the packet is received) are stored in Address Table, by way of "learning" an SA and its corresponding port. Inter-LAN connection equipment configures the interface port toward LAN 10 as the "a second port" for those packets from LAN 10. Therefore, when the packet is received via configured port LAN 10, the Inter-LAN connection equipment will have an intelligent to determine whether the packet is valid. Therefore, it is clear that Inter-LAN connection equipment has a mechanism to identify the configured port, which is a port where packets are provisioned to receive),

the processor further configured to provide packet handling when the first port is different from the second port (see col. 9, line 15-34; note that after comparing between the stored LAN port number in the memory table and the received packet's LAN port number, the packet is forwarded if they do not coincide.)

However, this limitation is taught by Sugiyama '547. Sugiyama '547 teaches a mechanism for processing a receiving packet at different ports. Khansari '131 teaches discarding erroneous packet when received port is not the same. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Khansari '131 as taught by Sugiyama '547 for the purpose of providing an inter-LAN connection equipment which can fastly start the forward of a packet to be passed and enhance a communication performance among terminals; see Sugiyama '547 col. 1, line 64-67. The motivation being that by providing an interconnect switch to handle erroneous packet arriving at different port before it forwards to the next switch, it can increase optimal network connectivity and performance.

Regarding claim 12, Khansari '131 discloses a plurality of link state update packets and a plurality of routing update packets (see col. 3, line 41-51 and see col. 5, line 54-62; per Fig. 4, the packet (i.e. MAC frame) consists of DA 102 and SA 104 fields, where each field can used to broadcast, unicast, or multicast to all bridges in the network regarding the routing/switching information. Broadcast Frame can be sent in response to new/updated switch/line/path information, or unicast frame can be sent in response to path/line failure by instructing a remote switch to update the routing.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Khansari '131 as taught by Sugiyama '547 for the same reason stated in Claim 10 above.

Regarding claim 13, Khansari '131 discloses one or more routing trees stored in the routing database in order to route the packet over the network as described above in Claim 10. Furthermore, Sugiyama '547 discloses the second port is calculated by examining the database (see Sugiyama '547 col. 2, line 4-20 and col. 4, line 33-67; note that each received packet's source address (SA) and its corresponding LAN port address (i.e. the port where the packet is received) are stored in Address Table, by way of "learning" an SA and its corresponding port. Inter-LAN connection equipment configures the interface port toward LAN 10 as the "a second port" for those packets from LAN 10. Thus, the configured port is determined by storing. Also, see Khansari '131 col. 8, line 30-45. Therefore, it is clear that before the port information is stored in the database/memory, it must be examined to ensure if there is any previous information install. If there is any information, the database will be updated.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Khansari '131 as taught by Sugiyama '547 for the same reason stated in Claim 10 above.

Regarding claim 14, Khansari '131 discloses second port is calculated by examining the source network address of the packet as described above in Claim 10.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Khansari '131 as taught by Sugiyama '547 for the same reason stated in Claim 10 above.

Regarding claim 18, Sugiyama '547 discloses spurious network traffic handling includes discarding the packet (Sugiyama '547 Fig. 7, step 214; col. 6, line 60-64; note that a duplicate packet arrived at the switch is the faulty/erroneous packet, and it is discarded by the switch.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Khansari '131 as taught by Sugiyama '547 for the same reason stated in Claim 10 above.

8. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Khansari '131 and Sugiyama '547, as applied to claim 10 above, and further in view of Spiegel (U.S. 5,649,108).

Regarding claim 11, the combined system of Khansari '131 and Sugiyama '547 discloses a routing database and a plurality of connected switches as described above in Claim 10.

Neither Khansari '131 nor Sugiyama '547 explicitly discloses a routing tree for each switch. (See Spiegel '108 Fig.1, connected switches A-G; and Fig. 2, Routing Table 13 at each switch; col. 6, line 37-67; note that each switch consists a routing table.)

However, this limitation is taught by Spiegel '108. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Khansari '131 and Sugiyama '547, as taught by Spiegel '108, for the purpose of providing the best alternate paths, or the paths with the least total cost if link-state protocols are used; see Spiegel '108 col. 2, line 24-25. The motivation being that by utilizing routing information stored routing table, it can increase the reliability in the network.

9. Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sugiyama '547 and Khansari '131, as applied to claim 10 above, and further in view of Dobbins (U.S. 5,946,308).

Regarding claim 15, the combined system Sugiyama '547 and Khansari '131 discloses processor as described above in Claim 10.

Neither Sugiyama '547 nor Khansari '131 explicitly discloses generating an expected port table (see Dobbins '308 Fig.6 and Fig. 7, Table 1, VLAN mapping for Switch 11),

the expected port table mapping each of a plurality of possible source network addresses (see Dobbins '308 Table 1, VLAN IDs: VLAN 100 and 200) to a unique port of the switch (see Dobbins '308 Table 1, access port 2),

whereby the second port is calculated by using a source network address of the packet (see Dobbins '308 col. 6, line 46-59; note that each switch strip off the encapsulated VLAN header to identify VLAN address) to look up the second port (see Dobbins '308 col. 7, line 13-40; note that each access port is configured/determined by mapping to at least one or more corresponding VLAN. Thus, when the packet arrives at the port, the table is used to

identify which VLAN does the packet belong, and the table validates whether the access port is the configured port to received packet.).

However, this limitation is taught by Dobbins '308. The combined system of Sugiyama '547 and Khansari '131 teaches Inter-LAN connection equipment that has an intelligent of which port a packet should receive. Dobbins '308 teaches that utilizing an SEFS switch with plurality of configured ports and ability to receive packets from various network/switches over the network where there are plurality of switches. Thus, the combined system of Sugiyama '547 and Khansari '131 can be used in Dobbins '308 network. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Khansari '131 and Sugiyama '547, as taught by Dobbins '308, for the purpose of designing a new secure fast packet switching (SFPS) technology which provides the same or better reliability and security as routers, but with much greater performance and without an increase in cost; see Dobbins '308 col. 1, line 44-55. The motivation being that by utilizing an SEFS switch in the network, it can increase the ability to guarantee a quality of service (QOS) by providing dedicated switched paths through the network via dedicated ports.

Regarding claim 16, the combined system Sugiyama '547 and Khansari '131 discloses a processor as described above in Claim 10.

Neither Sugiyama '547 nor Khansari '131 explicitly discloses generating an expected port table (see Dobbins '308 Fig.6 and Fig. 7, Table 1, VLAN mapping for Switch 11),

the expected port table mapping each of a plurality of possible source network addresses (see Dobbins '308 Table 2, VLAN IDs: VLAN 100 and 20) to a plurality of possible ports of the switch (see Dobbins '308 Table 2, access ports 1-2),

whereby a plurality of possible second ports are calculated by using a source network address of the packet (see Dobbins '308 col. 6, line 46-59; note that each switch strip off the encapsulated VLAN header to identify VLAN address; see also col. 7, line 13-40; note that each access port is configured/determined by mapping to at least one or more corresponding VLAN. Thus, when the packet arrives at the port, the table is used to identify which VLAN does the packet belong, and the table validates whether the access port is the configured port to received a packet. Also see Dobbins '308 Fig. 1 network consists of SFPS switches and Fig. 3 a logical view of an SFPS switch; see col. 4, line 21 to col. 5, line 41; note that SEFS switches in Fig. 1 has plurality of input and output ports and each port is connected to either plurality of network sides (label N) or access sides (i.e. user side/customer side with label A). In particular an SEFS switch S3 has four network ports connecting to other switches (i.e. S1 to S6). Therefore, an SEFS switch can be configured to receive a packet at any ports in from other switches based upon network and routing topology (i.e. a plurality of possible ports of the switch). Since there are pluralities of ports, pluralities of processes occur utilizing a VLAN address of received packets at each port.)

However, this limitation is taught by Dobbins '308. The combined system of Sugiyama '547 and Khansari '131 teaches Inter-LAN connection equipment that has an intelligent of which port a packet should receive. Dobbins '308 teaches that utilizing an SEFS switch with plurality of configured ports and ability to receive packets from various

network/switches over the network where there are plurality of switches. Thus, the combined system of Sugiyama '547 and Khansari '131 can be used in Dobbins '308 network. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined system of Khansari '131 and Sugiyama '547, as taught by Dobbins '308, for the purpose of designing a new secure fast packet switching (SFPS) technology which provides the same or better reliability and security as routers, but with much greater performance and without an increase in cost; see Dobbins '308 col. 1, line 44-55. The motivation being that by utilizing an SEFS switch in the network, it can increase the ability to guarantee a quality of service (QOS) by providing dedicated switched paths through the network via dedicated ports.

10. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Khansari '131 and Sugiyama '547, as applied to claim 10 above, and further in view of Miklos (U.S. 6,621,796).

Regarding claim 19, the combined system Khansari '131 and Sugiyama '547 discloses handling the spurious network traffic handling as described above in Claim 10.

Neither Sugiyama '547 nor Khansari '131 explicitly discloses generating an alert (see Miklos'796 Fig. 4 and col. 15, line 45-62; note that after the sender discards the packet, it generates a discard-signaling PDU message to notify the receiver which PDU has been discarded.)

However, this limitation is taught by Miklos'796. Therefore, it would have been obvious to one having ordinary skill in the art at the time the inventio0n was made to modify the combined system of Khansari '131 and Sugiyama '547, as taught by Miklos'796, for the

purpose of providing a sender-initiated discard mechanism that is specifically designed to operate efficiently and effectively with Selective Repeat ARQ; see Miklos'796 col. 2, line 55-61. The motivation being that by notifying the receiver regarding the discarded PDU, it can increase efficiency and reliability in the network.

11. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Khansari '131 in view of Sugiyama '547.

Regarding claim 20, Khansari '131 discloses an internetwork (see Fig. 2a, internetwork between LAN 1 and LAN 3) comprising a plurality of switches (see Fig. 2a, Bridges 16, 14, and 12), each of the switches comprising:

a plurality of ports (see Fig. 5, ports A1, B1, and C1), each port connected in a communicating relationship with at least one of a connected switch (see Fig.2a, Bridge 14) and a network (see Fig. 2a, network 10);

a routing database (see Fig. 5, Memory 52), the routing database containing information relating to the internetwork (see col. 6, line 1-59; see Fig. 5, Memory 52 contains a program, filtering database, and hash table 58; note that memory contains a database to store/learn reading address information regarding the packets to be switched/routed between internetwork); a processor (see Fig. 5, Controller 50), and whereby spurious network traffic within the inernetwork is detected. (See Fig. 7, step 214; col. 6, line 60-64; note that a duplicate packet arrived at the switch is the faulty/erroneous network traffic/packet, and it is discarded by the switch since the received ports are not the same).

Khansari '131 does not explicitly disclose the processor configured to compare a first port to a second port (see Fig. 1, LAN port Address Comparing CKT 46 and Terminal Address Comparing CKT 47; see col. 2, line 22-34 and see col. 5, line 29-53; note that when the packet is received at any port, the comparing circuits determine the validity of a packet by comparing between receiving port and learned port. In particular, a received packet's source address, destination address and the "first" received LAN port number are compared against the information (i.e. information including a second port number) stored in Filtering Address Table memory (or) learned memory. When the packet is received at a port, Inter-LAN connection equipment determines the validity of a packet regarding receiving port number and expected port number. Therefore, it is clear that Inter-LAN connection equipment has a mechanism to identify the receiving port, which is a port where packets are arriving), and

the first port being a one of the plurality of ports through which a packet is received (see col. 2, line 22-34 and see col. 5, line 29-53; note that any port (i.e. LAN 10 port, LAN20 port, or LAN 30 port) can receive a packet, and the receiving port is the "first" port), and

the second port being a one of the plurality of ports through which the packet is expected to received (see Fig. 1, Address Learning CKT 57; see col. 2, line 4-20 and col. 4, line 33-67; note that each received packet's source address (SA) and its corresponding LAN port address (i.e. the port where the packet is received) are stored in Address Table, by way of "learning" an SA and its corresponding port. Inter-LAN connection equipment configures the interface port toward LAN 10 as the "a second port" for those packets from LAN 10. Therefore, when the packet is received via configured port LAN 10, the Inter-LAN

connection equipment will have an intelligent to determine whether the packet is valid. Therefore, it is clear that Inter-LAN connection equipment has a mechanism to identify the configured port, which is a port where packets are provisioned to receive),

the processor further configured to provide packet handling when the first port is different from the second port (see col. 9, line 15-34; note that after comparing between the stored LAN port number in the memory table and the received packet's LAN port number, the packet is forwarded if they do not coincide.)

However, this limitation is taught by Sugiyama '547. Sugiyama '547 teaches a mechanism for processing a receiving packet at different ports. Khansari '131 teaches discarding erroneous packet when received port is not the same. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Khansari '131 as taught by Sugiyama '547 for the purpose of providing an inter-LAN connection equipment which can fastly start the forward of a packet to be passed and enhance a communication performance among terminals; see Sugiyama '547 col. 1, line 64-67. The motivation being that by providing an interconnect switch to handle erroneous packet arriving at different port before it forwards to the next switch, it can increase optimal network connectivity and performance.

Allowable Subject Matter

12. Claim 17 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Notes/Remarks

13. Objections to the drawings are withdrawn.

14. Claims objections are withdrawn.

15. Claim rejections under 35 USC § 112, second paragraph, on claims 1 and 6 are withdrawn since they are being amended accordingly.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ian N Moore whose telephone number is 703-605-1531. The examiner can normally be reached on M-F: 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ken Vanderpuye can be reached on 703-308-7828. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

INM
7/26/04

KENNETH VANDERPUYE
PRIMARY EXAMINER